The following is claimed:

1. Software from computer-readable medium(s) creating the signature portion of a user login account, as at least part of a subsequent validation protocol for login submission, wherein at least part of said signature having at least one user-determined transmission type.

2. Software from computer-readable medium(s) validating a signature comprising a plurality of signals by accessing data from a plurality of keys.

3. Software from computer-readable medium(s) incrementally validating a signature.

4. A method in software for creating the signature portion of a user login account, comprising at least one transmission, as at least part of a subsequent validation protocol for login submission, comprising the following steps:
a) a user determining transmission type of at least one transmission;
b) recording a plurality of signal types for at least one transmission;
c) packaging at least one recorded transmission into at least one key;
d) storing at least one key in at least one file.

5. A method in software for validating user login submission input data comprising the following steps:
a) accumulating possible keys based upon matching key data to initial input data;
b) discarding accumulated keys based upon failure to match to subsequent input data until validation is completed or by process of elimination impossible.

6. Software according to claim 1 whereby said user determining at least one signal type of at least one transmission of said signature.

7. Software according to claim 6 whereby said user-determined signal type is of a user-determined transmission type.

8. Software according to claim 1 wherein said signature comprising the entirety of login submission.

9. Software according to claim 2 wherein said validating by accessing data from a plurality of keys stored in one or more files, wherein said keys are in storage locations not contiguous.

10. Software according to claim 9 wherein said keys are stored in the same file.

11. Software according to claim 2 wherein said keys are stored in different files.

12. Software according to claim 2 employing at least one next key trajectory as part of said validating.

13. Software according to claim 3 wherein said validating comprising signal matching, whereby said matching may be successful with an inexact match between stored data and corresponding login submitted input data.

14. Software according to claim 3 whereby said validating terminating passively.

15. Software according to claim 14 wherein said terminating passively having been user determined during creation of said signature validation protocol.

16. The method according to claim 4 whereby said user determining at least one signal type of at least one transmission for said subsequent validation.

17. The method according to claim 4 whereby said user determining a plurality of transmission types from a plurality of said recorded transmissions.

18. The method according to claim 4 whereby recording a plurality of signal types emanating from a single transmission.

19. Software according to claim 4 storing at least one fake key.

20. The method according to claim 4 wherein packaging at least one next key trajectory in said key.

21. The method according to claim 4 wherein packaging a plurality of next key trajectories in said key.

22. The method according to claim 21 whereby said different next key trajectories are to keys in different files.

23. The method according to claim 4 wherein at least one transmission comprising input from a plurality of devices.